Brain Dump PECB ISO-IEC-27001-Lead-Auditor Free & New ISO-IEC-27001-Lead-Auditor Test Papers

2026 Latest DumpsTorrent ISO-IEC-27001-Lead-Auditor PDF Dumps and ISO-IEC-27001-Lead-Auditor Exam Engine Free Share: https://drive.google.com/open?id=1freH1-dMxje7hdrs7--vFNpu_Yosqjck

Our top priority is to help every customer in cracking the PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) test. Therefore, we have created these formats so that every applicant can prepare successfully for the PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) exam on the first attempt. We are aware that the cost for the registration of the PECB ISO-IEC-27001-Lead-Auditor examination is not what everyone can pay. After paying the hefty PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) test registration fee, applicants usually run on a tight budget. This is why DumpsTorrent provides you with the PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) real questions with up to 1 year of free updates.

PECB ISO-IEC-27001-Lead-Auditor Exam Syllabus Topics:

Section	Weight	Objectives
Fundamental Concepts of Information Security	15%	- Overview of ISO/IEC 27000 family of standards • 1. Structure and scope of ISO/IEC 27000 series • 2. Relationship between ISO/IEC 27001 and other standards - Information security principles and definitions • 1. Risk management fundamentals • 2. Confidentiality, integrity, availability

Auditing Principles and Practices	30%	- Audit concepts and principles • 1. Audit types and objectives • 2. Independence, objectivity and evidence-based approach - Audit preparation and planning • 1. Development of audit plan and checklist • 2. Defining audit scope, criteria and methodology - Audit reporting and follow-up • 1. Structure and content of audit report • 2. Corrective action verification and closure - Audit execution • 1. Conducting interviews and document reviews • 2. Identifying nonconformities and opportunities for improvement • 3. Collecting and verifying audit evidence
Requirements of ISO/IEC 27001:2022	30%	- General requirements and ISMS scope definition • 1. Determining ISMS boundaries and applicability • 2. Understanding the organization and its context - Support, operation, performance evaluation and improvement • 1. Resource management and competence • 2. Corrective action and continual improvement • 3. Internal audit and management review - Leadership and planning • 1. Management commitment and policy establishment • 2. Information security objectives and risk treatment planning
Information Security Controls (ISO/IEC 27002:2022)	25%	- Control categories and implementation guidance • 1. Organizational controls • 2. Physical controls • 3. People controls • 4. Technological controls

Pass Guaranteed PECB - ISO-IEC-27001-Lead-Auditor - PECB Certified ISO/IEC 27001 Lead Auditor exam –Reliable Brain Dump Free

The ISO-IEC-27001-Lead-Auditor practice exam we offered is designed with the real questions that will help you in enhancing your knowledge about the ISO-IEC-27001-Lead-Auditor certification exam. Our online test engine will improve your ability to solve the difficulty of ISO-IEC-27001-Lead-Auditor Real Questions and get used to the atmosphere of the formal test. Our experts created the valid ISO-IEC-27001-Lead-Auditor study guide for most of candidates to help them get good result with less time and money.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q407-Q412):

NEW QUESTION # 407

Scenario 7: Lawsy is a leading law firm with offices in New Jersey and New York City. It has over 50 attorneys offering sophisticated legal services to clients in business and commercial law, intellectual property, banking, and financial services. They believe they have a comfortable position in the market thanks to their commitment to implement information security best practices and remain up to date with technological developments.
Lawsy has implemented, evaluated, and conducted internal audits for an ISMS rigorously for two years now.
Now, they have applied for ISO/IEC 27001 certification to ISMA, a well-known and trusted certification body.
During stage 1 audit, the audit team reviewed all the ISMS documents created during the implementation.
They also reviewed and evaluated the records from management reviews and internal audits.
Lawsy submitted records of evidence that corrective actions on nonconformities were performed when necessary, so the audit team interviewed the internal auditor. The interview validated the adequacy and frequency of the internal audits by providing detailed insight into the internal audit plan and procedures.
The audit team continued with the verification of strategic documents, including the information security policy and risk evaluation criteria. During the information security policy review, the team noticed inconsistencies between the documented information describing governance framework (i.e., the information security policy) and the procedures.
Although the employees were allowed to take the laptops outside the workplace, Lawsy did not have procedures in place regarding the use of laptops in such cases. The policy only provided general information about the use of laptops. The company relied on employees' common knowledge to protect the confidentiality and integrity of information stored in the laptops. This issue was documented in the stage 1 audit report.
Upon completing stage 1 audit, the audit team leader prepared the audit plan, which addressed the audit objectives, scope, criteria, and procedures.
During stage 2 audit, the audit team interviewed the information security manager, who drafted the information security policy. He justified the Issue identified in stage 1 by stating that Lawsy conducts mandatory information security training and awareness sessions every three months.
Following the interview, the audit team examined 15 employee training records (out of 50) and concluded that Lawsy meets requirements of ISO/IEC 27001 related to training and awareness. To support this conclusion, they photocopied the examined employee training records.
Based on the scenario above, answer the following question:
Lawsy lacks a procedure regarding the use of laptops outside the workplace and it relies on employees' common knowledge to protect the confidentiality of information stored in the laptops. This presents:

- A. A nonconformity
- B. A conformity
- C. An anomaly

Answer: A

Explanation:
Lawsy's lack of specific procedures for the use of laptops outside the workplace, despite allowing such use, represents a nonconformity. ISO/IEC 27001 requires that security controls and management processes be clearly defined, documented, and implemented. Relying solely on employees' common knowledge does not fulfill the standard's requirements for managing information security risks associated with mobile and teleworking.
References: ISO/IEC 27001:2013, Clause A.6.2 (Mobile device and teleworking management)

NEW QUESTION # 408
Which of the following is an information security management system standard published by the International Organization for Standardization?

- A. ISO5501
- B. ISO22301
- C. ISO27001
- D. ISO9008

Answer: C

Explanation:
Explanation
ISO/IEC 27001:2022 is an information security management system standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the

organization. The standard is intended to be applicable to all organizations, regardless of type, size or nature. ISO/IEC 27001:2022 is part of the ISO/IEC 27000 family of standards, which provide a comprehensive framework for information security management. References: [CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course], ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC 27000 family - Information security management systems

NEW QUESTION # 409
You are performing an ISMS audit at a residential nursing home that provides healthcare services.
The next step in your audit plan is to verify the information security incident management process.
The IT Security Manager presents the information security incident management procedure (Document reference ID:ISMS_L2_16, version 4).
You review the document and notice a statement "Any information security weakness, event, and incident should be reported to the Point of Contact (PoC) within 1 hour after identification". When interviewing staff, you found that there were differences in the understanding of the meaning of the phrase "weakness, event, and incident".
The IT Security Manager explained that an online "information security handling" training seminar was conducted 6 months ago. All the people interviewed participated in and passed the reporting exercise and course assessment.
You would like to investigate other areas further to collect more audit evidence. Select three options that would not be valid audit trails.

- A. Collect more evidence on how the organisation learns from information security incidents and makes improvements. (Relevant to control A.5.27)
- B. Collect more evidence on how the organisation conducts information security incident training and evaluates its effectiveness. (Relevant to clause 7.2)
- C. Collect more evidence on how the organisation tests the business continuity plan. (Relevant to control A.5.30)
- D. Collect more evidence on how areas subject to information security incidents are quarantined to maintain information security during disruption (relevant to control A.5.29)
- E. Collect more evidence to determine if ISO 27035 (Information security incident management) is used as internal audit criteria. (Relevant to clause 8.13)
- F. Collect more evidence on how information security incidents are reported via appropriate channels (relevant to control A.6.8)
- G. Collect more evidence on whether terms and definitions are contained in the information security policy. (Relevant to control 5.32)
- H. Collect more evidence on how the organisation manages the Point of Contact (PoC) which monitors vulnerabilities. (Relevant to clause 8.1)

Answer: E,G,H

Explanation:
The three options that would not be valid audit trails are:
*Collect more evidence on how the organisation manages the Point of Contact (PoC) which monitors vulnerabilities. (Relevant to clause 8.1)
*Collect more evidence on whether terms and definitions are contained in the information security policy.
(Relevant to control 5.32)
*Collect more evidence to determine if ISO 27035 (Information security incident management) is used as internal audit criteria.
(Relevant to clause 8.13) These options are not valid audit trails because they are not directly related to the information security incident management process, which is the focus of the audit. The audit trails should be relevant to the objectives, scope, and criteria of the audit, and should provide sufficient and reliable evidence to support the audit findings and conclusions1.
Option E is not valid because the PoC is not a part of the information security incident management process, but rather a role that is responsible for reporting and escalating information security incidents to the appropriate authorities2. The audit trail should focus on how the PoC performs this function, not how the organisation manages the PoC.
Option G is not valid because the terms and definitions are not a part of the information security incident management process, but rather a part of the information security policy, which is a high-level document that defines the organisation's information security objectives, principles, and responsibilities3. The audit trail should focus on how the information security policy is communicated, implemented, and reviewed, not whether it contains terms and definitions.
Option H is not valid because ISO 27035 is not a part of the information security incident management process, but rather a guidance document that provides best practices for managing information security incidents4. The audit trail should focus on how the organisation follows the requirements of ISO/IEC 27001:
2022 for information security incident management, not whether it uses ISO 27035 as an internal audit criteria.
The other options are valid audit trails because they are related to the information security incident management process, and they can provide useful evidence to evaluate the conformity and effectiveness of the process. For example:

*Option A is valid because it relates to control A.5.29, which requires the organisation to establish procedures to isolate and quarantine areas subject to information security incidents, in order to prevent further damage and preserve evidence5. The audit trail should collect evidence on how the organisation implements and tests these procedures, and how they ensure the continuity of information security during disruption.
*Option B is valid because it relates to control A.6.8, which requires the organisation to establish mechanisms for reporting information security events and weaknesses, and to ensure that they are communicated in a timely manner to the appropriate levels within the organisation6. The audit trail should collect evidence on how the organisation defines and uses these mechanisms, and how they monitor and review the reporting process.
*Option C is valid because it relates to clause 7.2, which requires the organisation to provide information security awareness, education, and training to all persons under its control, and to evaluate the effectiveness of these activities7. The audit trail should collect evidence on how the organisation identifies the information security training needs, how they deliver and record the training, and how they measure the learning outcomes and feedback.
*Option D is valid because it relates to control A.5.27, which requires the organisation to learn from information security incidents and to implement corrective actions to prevent recurrence or reduce impact8.
The audit trail should collect evidence on how the organisation analyses and documents the root causes and consequences of information security incidents, how they identify and implement corrective actions, and how they verify the effectiveness of these actions.
*Option F is valid because it relates to control A.5.30, which requires the organisation to establish and maintain a business continuity plan to ensure the availability of information and information processing facilities in the event of a severe information security incident9. The audit trail should collect evidence on how the organisation develops and updates the business continuity plan, how they test and review the plan, and how they communicate and train the relevant personnel on the plan.
References:
1: ISO 19011:2018, 6.2;
2: ISO/IEC 27001:2022, A.6.8.1;
3: ISO/IEC 27001:2022, 5.2;
4: ISO/IEC 27035:2016, Introduction;
5: ISO/IEC 27001:2022, A.5.29;
6: ISO/IEC 27001:2022, A.6.8;
7: ISO/IEC 27001:2022, 7.2;
8: ISO/IEC 27001:2022, A.5.27;
9: ISO/IEC 27001:2022, A.5.30;
10: ISO 19011:2018;
11: ISO/IEC 27001:2022;
12: ISO/IEC 27001:2022;
13: ISO/IEC 27035:2016;
14: ISO/IEC 27001:2022;
15: ISO/IEC 27001:2022;
16: ISO/IEC 27001:2022;
17: ISO/IEC 27001:2022;
18: ISO/IEC 27001:2022

NEW QUESTION # 410
How is the purpose of information security policy best described?

- A. An information security policy documents the analysis of risks and the search for countermeasures.
- B. An information security policy provides direction and support to the management regarding information security.
- C. An information security policy makes the security plan concrete by providing it with the necessary details.
- D. An information security policy provides insight into threats and the possible consequences.

Answer: B

Explanation:
The purpose of information security policy is best described as providing direction and support to the management regarding information security. An information security policy is a high-level document that defines the organization's vision, objectives, principles and responsibilities for information security. It also sets the scope and context of the information security management system and aligns it with the organization's strategy and culture. An information security policy does not document the analysis of risks or the search for countermeasures, nor does it make the security plan concrete or provide insight into threats and consequences. These are tasks for other documents or processes within the information security management system. ISO/IEC 27001:2022 defines information security policy as "policy that provides direction and support for information security in accordance with business requirements and relevant laws and regulations" (see clause 3.29). Reference: [CQI & IRCA Certified ISO/IEC

27001:2022 Lead Auditor Training Course], ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, What is Information Security Policy?

NEW QUESTION # 411
Scenario 5
CyberShielding Systems Inc. provides security services spanning the entire information technology infrastructure. It provides cybersecurity software, including endpoint security, firewalls, and antivirus software. CyberShielding Systems Inc. has helped various companies secure their networks for two decades through advanced products and services. Having achieved a reputation in the information and network security sector, CyberShielding Systems Inc. decided to implement a security information management system (ISMS) based on ISO/IEC 27001 and obtain a certification to better secure its internal and customer assets and gain a competitive advantage.
The certification body initiated the process by selecting the audit team for CyberShielding Systems Inc.'s ISO /IEC 27001 certification. They provided the company with the name and background information of each audit member. However, upon review, CyberShielding Systems Inc. discovered that one of the auditors did not hold the security clearance required by them. Consequently, the company objected to the appointment of this auditor. Upon review, the certification body replaced the auditor in response to CyberShielding Systems Inc.'s objection.
As part of the audit process, CyberShielding Systems Inc.'s approach to risk and opportunity determination was assessed as a standalone activity. This involved examining the organization's methods for identifying and managing risks and opportunities. The audit team's core objectives encompassed providing assurance on the effectiveness of CyberShielding Systems Inc.'s risk and opportunity identification mechanisms and reviewing the organization's strategies for addressing these determined risks and opportunities. During this, the audit team also identified a risk due to a lack of oversight in the firewall configuration review process, where changes were implemented without proper approval, potentially exposing the company to vulnerabilities. This finding highlighted the need for stronger internal controls to prevent such issues.
The audit team accessed process descriptions and organizational charts to understand the main business processes and controls. They performed a limited analysis of the IT risks and controls because their access to the IT infrastructure and applications was limited by third-party service provider restrictions. However, the audit team stated that the risk of a significant defect occurring in CyberShielding's ISMS was low since most of the company's processes were automated. They therefore evaluated that the ISMS, as a whole, conforms to the standard requirements by questioning CyberShielding representatives on IT responsibilities, control effectiveness, and anti-malware measures. CyberShielding's representatives provided sufficient and appropriate evidence to address all these questions.
Despite the agreement signed before the audit, which outlined the audit scope, criteria, and objectives, the audit was primarily focused on assessing conformity with established criteria and ensuring compliance with statutory and regulatory requirements.
Question
Was the audit team's assessment of CyberShielding Systems Inc.'s risk and opportunity determination conducted in accordance with established auditing norms? Refer to Scenario 5.

- A. No, conducting standalone assessments is not recommended; it should be implicit during the entire audit of a management system.
- B. Yes, conducting the assessment independently is a recommended practice.
- C. No, unless CyberShielding Systems Inc. explicitly requested an independent assessment.

Answer: B

Explanation:
The audit team's approach to assessing risk and opportunity determination as a standalone activity is in line with established auditing norms, making option A the correct answer. ISO/IEC 27001:2022 requires organizations to identify risks and opportunities related to the ISMS and to plan actions to address them. From an audit perspective, ISO 19011 allows auditors to structure audit activities in a way that ensures effective coverage of critical requirements.
Assessing risk and opportunity determination independently does not violate auditing principles, provided it remains connected to the overall management system context. In practice, auditors often examine risk management as a distinct audit trail because it is a foundational element that influences many other ISMS processes, including control selection, operational planning, and continual improvement. Conducting a focused assessment enables auditors to evaluate whether risks are identified systematically, whether opportunities are considered, and whether treatment plans are appropriate and effective.
Option C is incorrect because although risk and opportunity management should be embedded throughout the ISMS, auditing it as a standalone activity does not contradict this principle. It is an audit structuring decision rather than a management system design issue.
Option B is incorrect because auditors do not require explicit auditee requests to structure audit activities independently; they are responsible for designing the audit approach.
Therefore, the audit team's standalone assessment of risk and opportunity determination aligns with recommended auditing practices.

NEW QUESTION # 412
.....

But our company can provide the anecdote for you--our ISO-IEC-27001-Lead-Auditor study materials. Under the guidance of our ISO-IEC-27001-Lead-Auditor exam practice, you can definitely pass the exam as well as getting the related certification with the minimum time and efforts. We would like to extend our sincere appreciation for you to browse our website, and we will never let you down. The advantages of our ISO-IEC-27001-Lead-Auditor Guide materials are more than you can imagine. Just rush to buy our ISO-IEC-27001-Lead-Auditor practice braindumps!

New ISO-IEC-27001-Lead-Auditor Test Papers: https://www.dumpstorrent.com/ISO-IEC-27001-Lead-Auditor-exam-dumps-torrent.html

- Reliable ISO-IEC-27001-Lead-Auditor Practice Questions □ ISO-IEC-27001-Lead-Auditor Review Guide □ ISO-IEC-27001-Lead-Auditor New Exam Camp □ Search for { ISO-IEC-27001-Lead-Auditor } and download it for free immediately on ⇒ www.validtorrent.com ⇐ □Reliable ISO-IEC-27001-Lead-Auditor Practice Questions
- 100% Pass 2026 Pass-Sure ISO-IEC-27001-Lead-Auditor: Brain Dump PECB Certified ISO/IEC 27001 Lead Auditor exam Free □ Search for ➽ ISO-IEC-27001-Lead-Auditor □ and obtain a free download on 【 www.pdfvce.com 】 ☮ISO-IEC-27001-Lead-Auditor New Dumps Book
- ISO-IEC-27001-Lead-Auditor Brain Dumps □ ISO-IEC-27001-Lead-Auditor Review Guide □ ISO-IEC-27001-Lead-Auditor Latest Test Experience □ Search for ➽ ISO-IEC-27001-Lead-Auditor □ and download exam materials for free through ➡ www.pdfdumps.com □□□ □ISO-IEC-27001-Lead-Auditor Certification Dumps
- Pass-Sure ISO-IEC-27001-Lead-Auditor - Brain Dump PECB Certified ISO/IEC 27001 Lead Auditor exam Free □ Download （ ISO-IEC-27001-Lead-Auditor ） for free by simply searching on 【 www.pdfvce.com 】 □ISO-IEC-27001-Lead-Auditor Review Guide
- ISO-IEC-27001-Lead-Auditor New Exam Camp □ ISO-IEC-27001-Lead-Auditor Reliable Test Prep □ ISO-IEC-27001-Lead-Auditor New Question □ Easily obtain free download of □ ISO-IEC-27001-Lead-Auditor □ by searching on □ www.prep4sures.top □ □ISO-IEC-27001-Lead-Auditor New Exam Camp
- ISO-IEC-27001-Lead-Auditor Review Guide □ ISO-IEC-27001-Lead-Auditor Exam Guide □ Practice Test ISO-IEC-27001-Lead-Auditor Fee □ Immediately open □ www.pdfvce.com □ and search for " ISO-IEC-27001-Lead-Auditor " to obtain a free download □ISO-IEC-27001-Lead-Auditor Exam Guide
- Authentic ISO-IEC-27001-Lead-Auditor exam materials: PECB Certified ISO/IEC 27001 Lead Auditor exam bring you the latest exam questions - www.practicevce.com □ Easily obtain free download of ✔ ISO-IEC-27001-Lead-Auditor □✔□ by searching on 【 www.practicevce.com 】 □ISO-IEC-27001-Lead-Auditor Exam Fees
- ISO-IEC-27001-Lead-Auditor Reliable Test Prep □ Exam ISO-IEC-27001-Lead-Auditor Pass4sure □ ISO-IEC-27001-Lead-Auditor New Exam Camp □ Search for 「 ISO-IEC-27001-Lead-Auditor 」 and download exam materials for free through （ www.pdfvce.com ） ▸Detailed ISO-IEC-27001-Lead-Auditor Answers
- Free ISO-IEC-27001-Lead-Auditor dumps torrent - ISO-IEC-27001-Lead-Auditor exams4sure pdf - PECB ISO-IEC-27001-Lead-Auditor pdf vce □ Download ➠ ISO-IEC-27001-Lead-Auditor □ for free by simply entering 《 www.dumpsquestion.com 》 website □ISO-IEC-27001-Lead-Auditor Latest Exam
- ISO-IEC-27001-Lead-Auditor exam collection guarantee ISO-IEC-27001-Lead-Auditor PECB Certified ISO/IEC 27001 Lead Auditor exam exam success □ Search for 「 ISO-IEC-27001-Lead-Auditor 」 on " www.pdfvce.com " immediately to obtain a free download □ISO-IEC-27001-Lead-Auditor Latest Exam
- ISO-IEC-27001-Lead-Auditor New Dumps Book □ Reliable ISO-IEC-27001-Lead-Auditor Practice Questions □ Valid ISO-IEC-27001-Lead-Auditor Exam Guide □ Search on 【 www.examcollectionpass.com 】 for □ ISO-IEC-27001-Lead-Auditor □ to obtain exam materials for free download □ISO-IEC-27001-Lead-Auditor Valid Exam Forum
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, fortunetelleroracle.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New ISO-IEC-27001-Lead-Auditor dumps are available on Google Drive shared by DumpsTorrent: https://drive.google.com/open?id=1freH1-dMxje7hdrs7--vFNpu_Yosqjck